UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,721	07/03/2003	Arben Kryeziu	1780.003US1	4980

21186 7590 08/26/2008
SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
08/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/613,721	KRYEZIU, ARBEN	
	Examiner	Art Unit	
	ELENI A. SHIFERAW	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 07/25/2008 has been entered.

Response to Amendment and Arguments

2. Applicant's amendments and arguments with respect to all amended independent claims have been fully considered but are not persuasive.

Regarding applicant's argument the none of the references disclosing wherein "the media player executes within a World-Wide Web browser", argument is not persuasive because McGarrahan refers Video On Demand content streaming/executing via a world wide web see par. 0033. Ishibashi et al. teaches different types of software content transmissions via internet network to a user see par. 0084 and 0101. Ishiguro et al. discloses music content distribution over a world wide network see fig. 1 and col. 4 lines 21-55. Spanga et al. teaches secure delivery of digital data and digital rights via network internet such as world wide web see col. 1 lines 32-39.

The examiner provides reference Nagahara US PG Pubs 2002/0091652 A1 for applicant's reference: transmission and execution of multimedia data via World Wide

Web browser is well-known at the time of the invention was made see par. 0132 wherein a user terminal 200 accessing/requesting/executing digital content via WWW browser.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1, 8, and 15 and dependent claims are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant referring to paragraphs from other application's disclosure that is not a provisional or a continuation to the current application but mentioned in the current application, is considered as new mater, to amendments done on 06/26/2008. See page 7 par. 1 of the remark submitted on 06/26/2008 and par. 0012 of the current application.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 1, 8, and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The use of the trademark "World-Wide Web" and "WWW" in the claims renders the claims indefinite. Perhaps "world wide web" or "www" was intended. Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGarrahan et al. US Pub. 20030026424 A1. in view of Ishibashi et al. 20010053223 A1 and Ishiguro et al. 7266691 B1.

As per claim 1, McGarrahan et al. method to authenticate a media stream recipient (0050-0055), comprising:

automatically receiving an authentication request from a media player when a recipient attempts to use the media player to play a media stream (0050-0051 and 0054), the media stream includes the media player and media content (0032-0033) and the media content is in a format known only to the media player (0054, 0047, 0051 and 0009 lines 11-13) and is not accessible to the recipient until the media player determines that the recipient is authenticated for access and the media player generates authentication information on behalf of the recipient and supplies that authentication information with

the authentication request (0053-0054; *STB requiring key from central billing system for user request*); and wherein the media player is self-loading and self-extracting from the streamed media stream within a computing environment of the recipient (0051; *user device STB displaying content stored with in STB based on authentication result upon user request*), and self-loads and executes when the recipient attempts to use the media player to play the media content (0051-0055) and wherein the media player executes within a World-Wide Web browser (0033);

verifying that the recipient is authorized to play the media content of the media stream (0051) in response to the media player supplied and generated authentication information (0053); and

sending an authentication token to the media player over a network connection, when if the recipient is authorized (0053), and wherein the media player automatically plays the media content stream once the authentication token is received by the media player, and wherein the authentication token serves as an electronic acknowledgement that it is okay to play the media content (0051).

McGarrahan et al. fails to explicitly disclose wherein when the recipient receives the media content via the media stream the recipient receives with that media stream the media player (*media player/software, according to applicant's remark on 12/12/09, received with content at the recipient*), as amended.

However it is well known to transmit a content with a software to let the receiver/recipient device know what kind of software has been used (*see Ishibashi et al. fig. 5 for algorithms for signature..., and see fig. 12 a single stream 1200 that contains*

content and digital signature comprising algorithm, and see par. 0112, and 0130-0132 for verifying and providing content using the received algorithm).

Therefore it would have been obvious at the time of the invention was made to modify the teachings of Ishibashi et al. within the system of McGarrahan et al. because they are analogous in secure method of providing content. One would have been motivated to modify the teachings because it would specify what kind of software has been used and authenticate using received algorithm.

The combination of McGarrahan et al. and Ishibashi et al. fail to explicitly disclose wherein the media player and media content temporarily reside in volatile memory of a recipient computing device associated with the recipient and once the media content is played for the recipient the media player and content are removed from volatile memory and no longer available on the recipient computing device thereby requiring the recipient to re-acquire the media content and media player each time the media content is played by the recipient.

However Ishiguro et al. discloses providing and storing content to user device flash memory for specified time and playing content only according to the specified time, and when the specified time ends deleting the content from the user devices flash memory (see col. 23 lines 10-33 and col. 8 lines 29-33) and requiring a re-authentication and re-acquiring content re-transmission each time the user tries to replay after deletion (see col. 29 lines 3-32).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Ishiguro et al. because they are analogous in content protection. One would have been motivated to incorporate the

teachings and modify it within the combination system because it would control content from being replayed illegally without controlled access.

As to claim 2, McGarrahan et al. discloses the method wherein the sending further comprises automatically installing the authentication token as a licensing key on a computing device of the recipient, wherein the licensing key can include licensing limitations (0053, 0055, and 0068).

As to claim 3, McGarrahan et al. discloses the method wherein in automatically receiving, the recipient initially obtains the media player and media stream from a second recipient (0048 and 0050).

As to claim 4, McGarrahan et al. discloses the method wherein in verifying, the recipient is verified by externally contacting a licensing service with at least one of an identity of the recipient and an identification of the media stream (0033-0034, 0067-0068).

As to claim 5, McGarrahan et al. discloses the method wherein in sending, the authentication token includes limitations that instruct the media player to self destruct the media stream upon the occurrence of an event or pre-defined time (0053-0055).

8. Claims 8-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGarrahan et al. US Pub. 20030026424 A1. in view of Ishibashi et al. 20010053223 A1 and Kempf et al.

Regarding claim 8 McGarrahan et al. discloses the media stream structure stored/embodied on a computer readable

medium, comprising:

media player logic (0046-0048);

media content (0046, 0032-0033, and 0051; *DTV signal/movie...*); and

media recipient authentication logic included within the media player logic (0051);

wherein when the media stream data structure is streamed to a computing device (0051), the media player logic is self-loading and self-installing on the computing device when a recipient associated with the computing device attempts to play the media content (0051-0055), and wherein the media player logic executes within a World-Wide Web (WWW) browser (0033), and media player logic executes the media recipient authentication logic before playing the media content by generating authentication information on behalf of the recipient, and wherein the media recipient authentication logic sends an authentication request having the authentication information to an authentication service over a network along with the identity of a the recipient of the media content, and wherein the media player logic automatically plays the media content when the authentication request is successful (0051-0054), and wherein the media content is in a format known only to the media player logic (0054, 0047, and 0051) and the media player logic only plays the media content when the recipient is successfully authenticated by the authentication service in response to the media player logic generated and supplied authentication information (0051-0054);

a valid license for media player logic is needed on the computing device before the media player logic can play the media content on the computing device for the recipient (0033-0034 and 0067).

McGarrahan et al. fails to explicitly disclose wherein when the recipient receives the media content via the media stream the recipient receives with that media stream the media player (*media player/software, according to applicant's remark on 12/12/09, received with content at the recipient*), as amended.

However it is well known to transmit a content with a software to let the receiver/recipient device know what kind of software has been used (*see Ishibashi et al. fig. 5 for algorithms for signature..., and see fig. 12 a single stream 1200 that contains content and digital signature comprising algorithm, and see par. 0112, and 0130-0132 for verifying and providing content using the received algorithm*) via internet network to a user (see par. 0084 and 0101).

Therefore it would have been obvious at the time of the invention was made to modify the teachings of Ishibashi et al. within the system of McGarrahan et al. because they are analogous in secure method of providing content. One would have been motivated to modify the teachings because it would specify what kind of software has been used and authenticate using received algorithm.

McGarrahan et al. and Ishibashi et al. fail to explicitly disclose wherein the media stream structure is encoded before it is streamed to the computing device with a security identification, the computing device also has a same security identification, and the security identification is based on an Internet Protocol (IP address of the computing device and the media content requires a match on the security identification of the media

stream structure with the security identification of the computing device before the media content is permitted to play.

However Kempf et al. discloses Identity Based Private Key generator (IPKG) generation a key (addressed based keys) using Internet Protocol address of a host and encrypting message data using the key for authentication and authorization (see par. 0013-0015) and/or network access (0038-0039). It would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Kempf et al. within the combination system because they are analogous in authentication and authorization and/or access control. One would have been motivated to modify the teachings because it would verify and/or compare IP address to provide access and/or secure communication.

As to claim 9, McGarrahan et al. discloses the media stream data structure wherein the media recipient
authentication logic also sends an identification of the media content to the authentication service (0051).

As to claim 10, McGarrahan et al. discloses the media stream data structure further comprising an authentication token, which is added to the media stream data structure if the identity of the recipient is authorized to play the media content on the computing device by the authentication service (0051-0055).

As to claim 11, McGarrahan et al. discloses the media stream data structure wherein the

authentication token is stored external to the media stream data structure and is identified within the media stream data structure as a pointer reference (0053-0054).

As to claim 12, McGarrahan et al. discloses the media stream data structure wherein the media recipient authentication logic also sends at least one of settings associated with a computing environment of the computing device and an Internet Protocol (IP) address associated with the computing device to the authentication service (0050054).

As to claim 13, McGarrahan et al. discloses the media stream data structure wherein the authentication service authenticates the identity of the recipient by interfacing with one or more external licensing services (0051, and 0068).

As to claim 14, McGarrahan et al. discloses the media stream data structure wherein the media player automatically plays the media content if a valid authentication token is received from the authentication service (0051 and 0054).

9. Claims 15-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGarrahan et al. US Pub. 20030026424 A1. in view of Ishibashi et al. 20010053223 A1 and Spagna et al. 6859791 B1.

Regarding claim 15, McGarrahan et al. teaches the media content authentication system, comprising:

a distribution service for distributing media streams via streaming to recipients (fig. 1), wherein each media stream includes media content (0046, 0032-0033, and 0051) and a self-installing, self-loading, and self-executing media player that is received and processes within a World-Wide Web browser (0033), the media content is in a format known only to the media player and the media player self-installs, self-loads, and self-executes when the recipients attempt to play the media content (0051; *user device STB displaying content stored with in STB based on authentication result upon user request*); and

an authentication service that subsequently communicates with each media player over a network in order to authenticate access to the recipients that attempts to play the media content (fig. 1 and 0054), and wherein each media player initiates the communication with the authentication service when it self-executes in an environment of a recipient to which it relates and each media player generates and supplies authentication information with the communication to the authentication service, the authentication information for a particular recipient to which a particular media player relates, and when authentication is successful each media player automatically plays media content included in the media stream (0051-0054).

One ordinary skill in the art would easily understand that authentication information of McGarrahan et al. is made of plurality of identifiers but fail to include few, Ishibashi et al. is disclosed for authentication information including identities for the recipients (*user ID*), identifications for the media content (*content ID*), identifications for the media streams, setting for each computing device's electronic environment, identifications for the media players (*encryption processing unit ID*), identifications for

any previous sender or previous recipient of the media streams, and identities for content providers that own the media stream (see fig. 16 of Ishibashi et al.).

McGarrahan et al. also fails to explicitly disclose wherein when the recipient receives the media content via the media stream the recipient receives with that media stream the media player (*media player/software, according to applicant's remark on 12/12/09, received with content at the recipient*), as amended.

However it is well known to transmit a content with a software to let the receiver/recipient device know what kind of software has been used (*see Ishibashi et al. fig. 5 for algorithms for signature..., and see fig. 12 a single stream 1200 that contains content and digital signature comprising algorithm, and see par. 0112, and 0130-0132 for verifying and providing content using the received algorithm*) using internet network to a user (see par. 0084 and 0101).

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Ishibashi within the system of McGarrahan et al. because they are analogous in content distribution. One would have been motivated to incorporate and modify the teachings, as Ishibashi suggests on 0204, to include any identification information for identification purpose in the authentication process.

Moreover, it would have been obvious at the time of the invention was made to modify the teachings of Ishibashi et al. within the system of McGarrahan et al. because they are analogous in secure method of providing content. One would have been motivated to modify the teachings because it would specify what kind of software has been used and authenticate using received algorithm.

Even though including any identifier within authentication information, such as an Internet Protocol (IP) addresses for computing devices of the recipients in the authentication information, is obvious to one ordinary skill in the art at the time of the invention, as explained above, the combination fails to disclose Internet Protocol (IP) addresses for computing devices of the recipients in the authentication information. However Spagna et al. is disclosed for receiving a content access request comprising IP address of the requester within authentication information and an authenticator comparing received IP address of the requestor with stored to provide the requested content access (see claim 16). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings within the combination system because it would control access to provide content.

As to claim 16, McGarrahan et al. discloses the media content authentication system wherein each media player that self-installs contacts the authentication service immediately after it initially installs on a recipient's computing device (0051-0054).

As to claim 17, McGarrahan et al. discloses the media content authentication system wherein each media player receives an authentication token from the authentication service, if a corresponding recipient is authorized to play the media content (0051-0054).

As to claim 18, McGarrahan et al. discloses the media content authentication system wherein the authentication service uses a licensing service to authorize a number of the recipients for access to the media content (0033-0034, 0067-0068).

As to claim 19, McGarrahan et al. discloses the media content authentication system wherein the

authentication service receives information from each of the media players that is used to authenticate each of the recipients, and the information includes at least one of settings of a computing environment that is executing the media player, an identity of the recipient, and an identification of the media content (0051-0054).

As to claim 20, McGarrahan et al. discloses the media content authentication system wherein the authentication service returns authentication tokens to each of the media players that have authorized recipients and the authentication tokens are at least one of a digital certificates, digital signatures, encrypted data, and hidden data (abstract; *encrypted...*).

10. Claim s 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGarrahan et al. US Pub. 20030026424 A1., Ishibashi et al. 20010053223 A1 and Ishiguro et al. 7266691 B1. and further in view of Yamasaki et al. US PUB. 2002/0161997 A1.

As to claim 6, the combination fails to disclose the method wherein in sending, the authentication token includes limitation that instruct the media player to prevent the recipient from re-streaming the media stream to a downstream recipient. However,

preventing authorized user receiver tamper resistant device from transmitting content/content key to other unauthorized person is disclosed by Yamasaki et al. par. 0055 and fig. 3. Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Yamasaki et al. within the system of McGarrahan et al. because they are analogous in content protection. One would have been motivated to do so because it would protect content from misappropriate use.

As to claim 7, Yamasaki et al. further discloses the method wherein in sending, the authentication token is at least one of a digital certificate and a digital signature (0015, 0042-0043, 0046 and 0048-0051). It would have been obvious to one having ordinary skill in the art at the time of the invention was made to use one of certificate/signature because it was very well known at the time of the invention to verify authorized content user in a system of content protection.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/
Examiner, Art Unit 2136